



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/415,293	10/08/1999	EARL T. CARTER	062891.0324	4623

7590 05/22/2003  
SCOTT T MORRIS  
BAKER & BOTTS LLP  
2001 ROSS AVENUE  
DALLAS, TX 752012980

EXAMINER

NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 05/22/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Tom Felger  
512/322-2599

# Office Action Summary

Application No.

09/415,293

Applicant(s)

CARTER, EARL T.

Examiner

Abdulhakim Nobahar

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☐ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

## Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2+3
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_

## DETAILED ACTION

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-5 and 7-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Hile et al. (5,319,776) (hereinafter Hile).

Referring to claims 1 and 7, Hile discloses:

“Maintaining a state table”. See, for example, column 2, lines 36-42.

“The state table indexed such that inputs comprising a current state and a current character yield an output of a new state, the new state related to an indication of an attack on a computer network”. See, for example, column 4, line 59-column 5, line 21 where the machine state at start is zero and every next state and every incoming

Art Unit: 2132

character are corresponding to the recited current state and current character, respectively, which are applied (inputted) to the state table to determine the next state of the machine. At the end, if checking of all characters of a string results in a predetermined machine state a virus match (intrusion detection) has occurred (indication of an attack).

“Maintaining the current state”. See, for example, Figure 3, where after each comparison step the resulting new state is maintained to be used as a current step for the next comparison step.

“Receiving an input stream, the input stream comprising a plurality of characters”. See, for example, column 4, lines 47-58.

“Selecting a first character of the input stream as the current character; and comparing a current character and the current state to the state table to generate a new state”. See, for example, column 4, line 66-column 5, line 20.

Referring to claim 2, Hile discloses:

“Initializing the current state to an initial state”. See, for example, column 4, lines 64-66.

Referring to claims 3 and 11, Hile discloses:

“Setting the current state equal to the new state; selecting a next character as the current character, the next character appearing subsequent to the first character in the

Art Unit: 2132

input stream; and repeating the comparing step". See, for example, column 4, line 59-  
column 5, line 21.

Referring to claims 4 and 12, Hile discloses:

"Recognizing the new state as indicative of an attack upon the computer  
network". See, for example, column 5, lines 17-21.

Referring to claim 5, Hile discloses:

"Sounding an alarm". See, for example, column 4, lines 16-22.

Referring to claim 8, Hile discloses:

"A computer readable medium, wherein the state table is stored upon the  
computer readable medium". See, for example, column 2, lines 4-7 and lines 36-42,  
column 3, lines 24-26 and column 4, lines 13-16.

Referring to claim 9, Hile discloses:

"The state machine comprises software code stored upon the computer readable  
medium, the software code further operable to be executed by a computer processor".  
See, for example, column 2, lines 36-42, column 4, lines 48-50 and column 5, lines 22-  
30.

Referring to claim 10, Hile discloses:

"The state machine is further operable to initialize the current state to an initial state". See, for example, column 4, lines 64-66.

Referring to claim 13, Hile discloses:

"A computer readable medium". See, for example, column 2, lines 4-7 and column 3, lines 24-26.

"A network interface for receiving an input stream comprising a plurality of characters". See, for example, column 1, lines 19-32.

"A processor communicatively coupled to the computer readable medium and the network interface". See, for example, column 2, lines 25-27 and lines 36-40, column 3, lines 17-24 and column 7, lines 39-44.

"A state table stored upon the computer readable medium, the state table indexed such that inputs comprising a current state and a current character yield an output of a new state, the new state related to an attack on a computer network". See, for example, column 4, lines 13-16 and column 4, line 59-column 5, line 21 where the machine state at start is zero and every next state and every incoming character are corresponding to the recited current state and current character, respectively, which are applied (inputted) to the state table to determine the next state of the machine. At the end, if checking of all characters of a string results in a predetermined machine state a virus match (intrusion detection) has occurred (indication of an attack).

"A state machine comprising instructions stored upon the computer readable medium and executable by the processor". See, for example, column 4, line 56-column 5, line 20.

"The state machine communicatively coupled to the state table". See, for example, column 2, line 36-42.

"The state machine operable to: maintain the current state". See, for example, Figure 3, where after each comparison step the resulting new state is maintained to be used as a current step for the next comparison step.

"Select a first character of the input stream as the current character and compare the current character and the current state to the state table to generate a new state". See, for example, column 4, line 66-column 5, line 20.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2132

Claim 6 is rejected under 35 USC 103(a) as being unpatentable over Hile et al. (5,319,776) (hereinafter Hile) in view of Ainsbury et al (6,078,924) (hereinafter Ainsbury).

Referring to claim 6, Hile does not expressly disclose:

"Generating the state table from a REGEX command". Ainsbury teaches that the REGEX (Regular Expression) are used to form tables. The Regular Expressions are commonly used in the art for parsing tables. See, for example, column 49, lines 57-67 and column 50, line 57-column 51, line 67.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the use of REGEX to generate state tables as taught in Ainsbury with the system of Hile, because it would provide state tables to be parsed by REGEX command to identify a pattern of character string.

69  
5/10/03 *Conclusion*  
PTD-1449 lacks several date entries. Applicant is requested to provide ~~the~~ ~~the~~ dates for the missing entries.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

U.S. Patent No. 5,375,248 to Lemay et al. teaches the use of state tables in a finite state machine for determining the next state by inputting the current state and an address, which corresponds to a character.



U.S. Patent No. 5,488,719 to Kaplan et al. teaches the use of a finite state machine and state tables for string matching.

U.S. Patent No. 4,450,520 to Hollaar et al. teaches a method for comparing an incoming sequential string against a pattern with arbitrary number of elements using state tables and a finite state machine.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Abdulhakim Nobahar  
Examiner  
Art Unit 2132

*A.N.*

AN  
May 16, 2003

*Gilberto B. J.*  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100